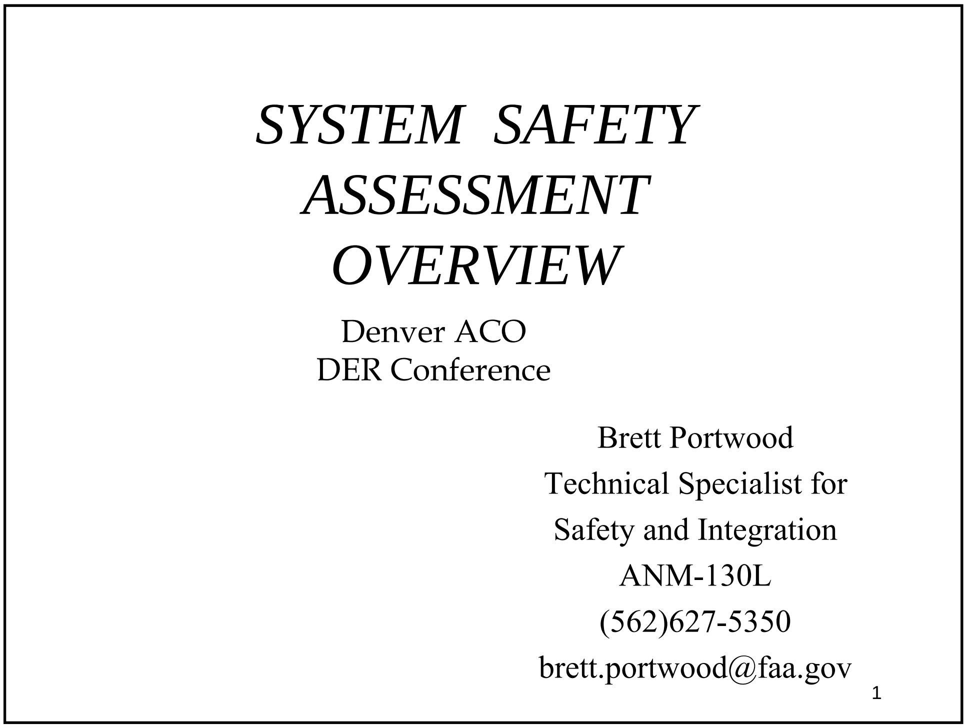
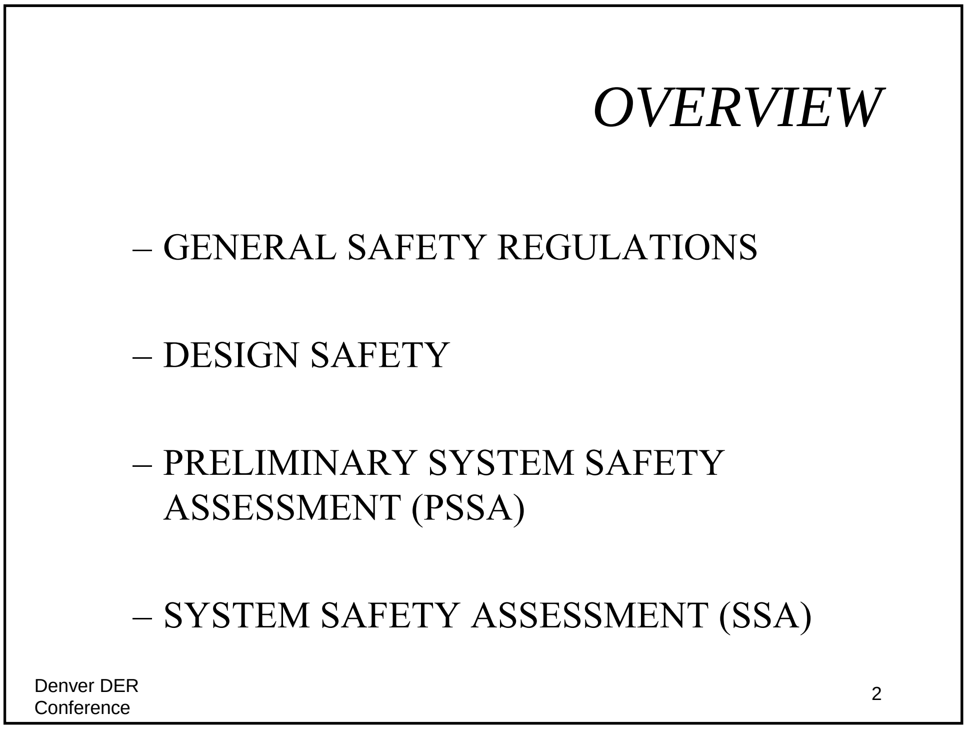


SYSTEM SAFETY ASSESSMENT OVERVIEW

Denver ACO
DER Conference

Brett Portwood
Technical Specialist for
Safety and Integration
ANM-130L
(562)627-5350
brett.portwood@faa.gov



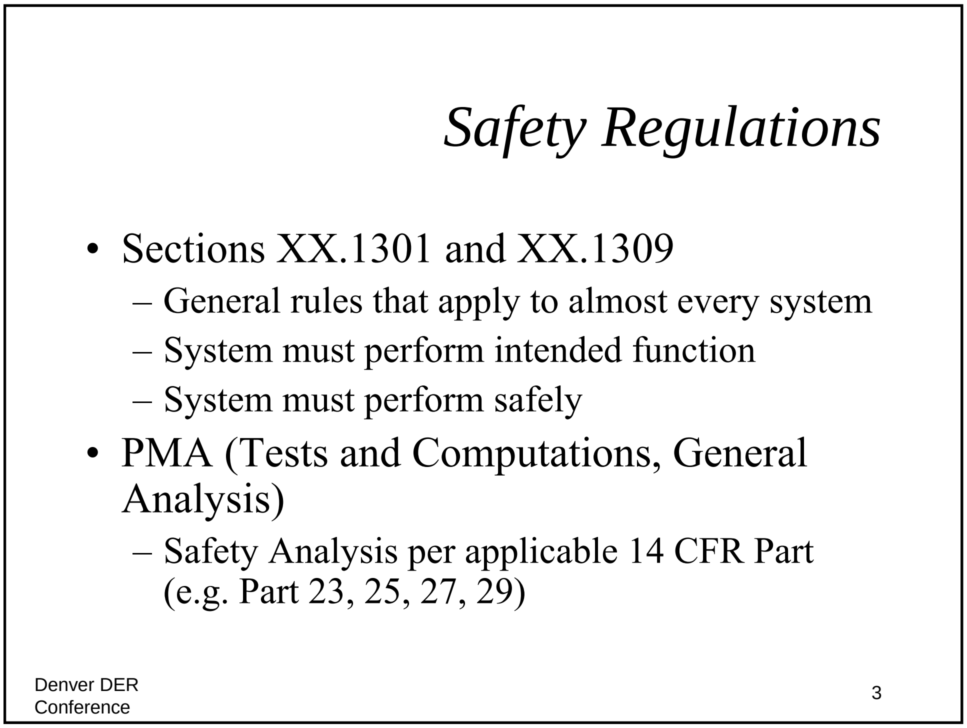
OVERVIEW

– GENERAL SAFETY REGULATIONS

– DESIGN SAFETY

– PRELIMINARY SYSTEM SAFETY ASSESSMENT (PSSA)

– SYSTEM SAFETY ASSESSMENT (SSA)

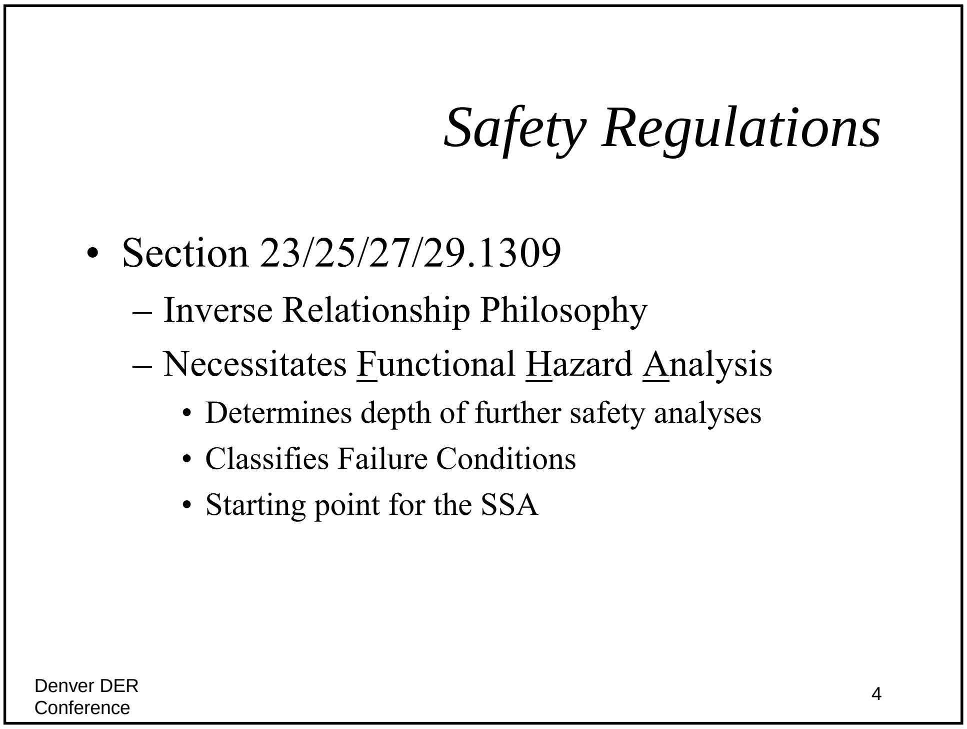


Safety Regulations

- Sections XX.1301 and XX.1309
  - General rules that apply to almost every system
  - System must perform intended function
  - System must perform safely
- PMA (Tests and Computations, General Analysis)
  - Safety Analysis per applicable 14 CFR Part (e.g. Part 23, 25, 27, 29)

Denver DER
Conference

3



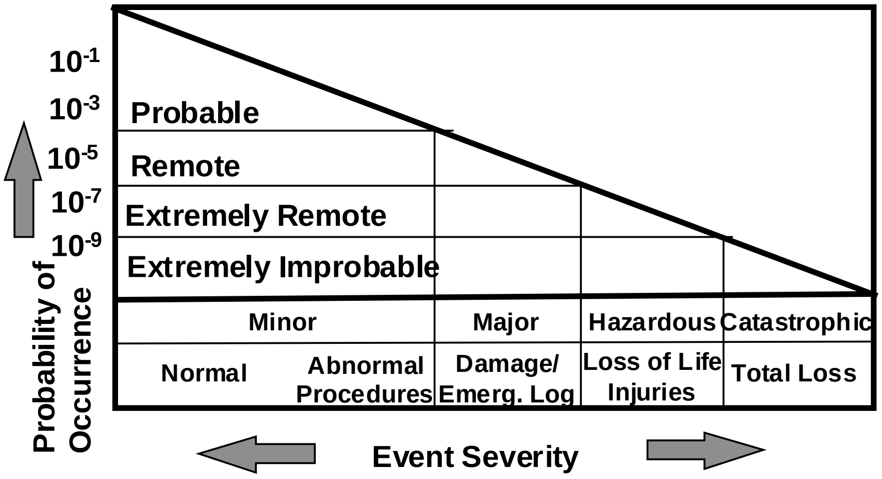
Safety Regulations

- Section 23/25/27/29.1309
  - Inverse Relationship Philosophy
  - Necessitates Functional Hazard Analysis
    - Determines depth of further safety analyses
    - Classifies Failure Conditions
    - Starting point for the SSA

Denver DER
Conference

4

Inverse Relationship Approach



Denver DER Conference

6 - 7 5

Hazard Severity Classes

- AC 25.1309-1A (1988)
  - 4 classes- Catastrophic, Severe-Major, Major, and Minor
- Since DO-178B and JAA harmonization
  - 5 classes- Catastrophic, Hazardous, Major, Minor and No Effect (Severe-Major became Hazardous and added a No effect category with no quantitative or qualitative probability requirements)

Denver DER Conference

6

Hazard Severity Classes (Part 25 Requirements)

(sheet 1 of 5)

Hazard Severity Classes *(sheet 2 of 5)*

Hazard Severity Classes *(sheet 3 of 5)*

Denver DER
Conference

9

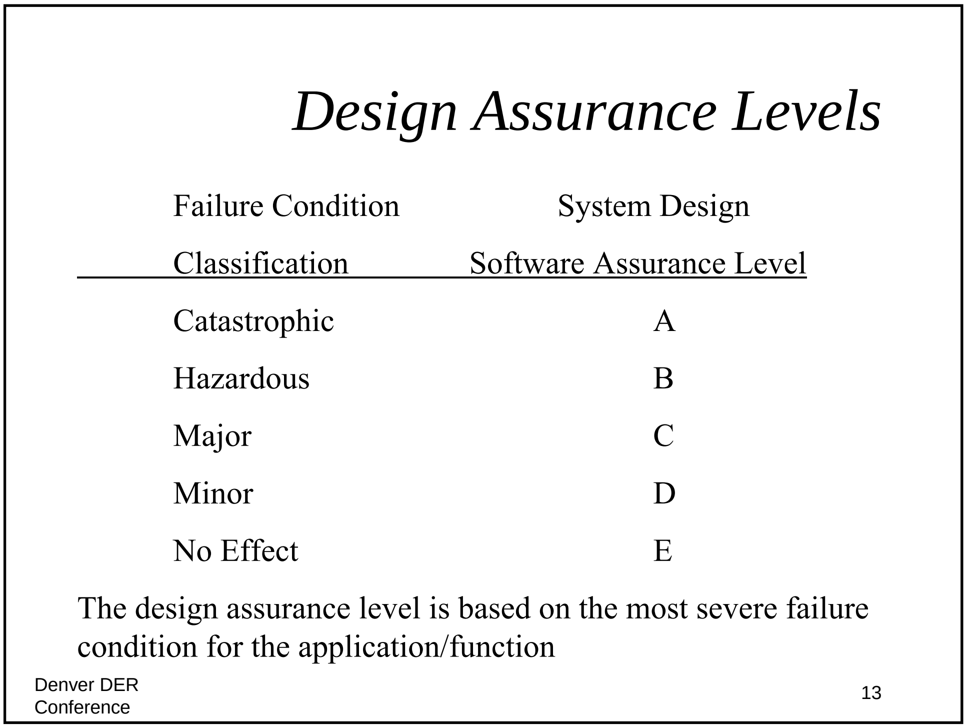
Hazard Severity Classes *(sheet 4 of 5)*

Denver DER
Conference

10

Hazard Severity Classes *(sheet 5 of 5)*

Part 23 Requirements (AC 25.1309-1C)



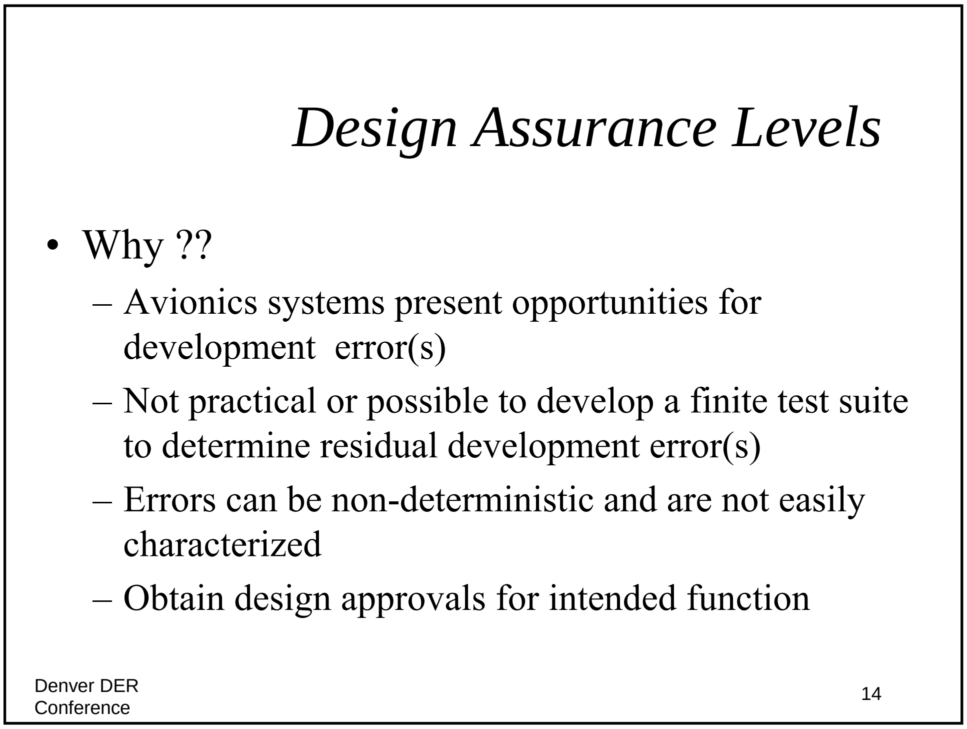
Design Assurance Levels

Failure Condition Classification	System Design Software Assurance Level
Catastrophic	A
Hazardous	B
Major	C
Minor	D
No Effect	E

The design assurance level is based on the most severe failure condition for the application/function

Denver DER
Conference

13

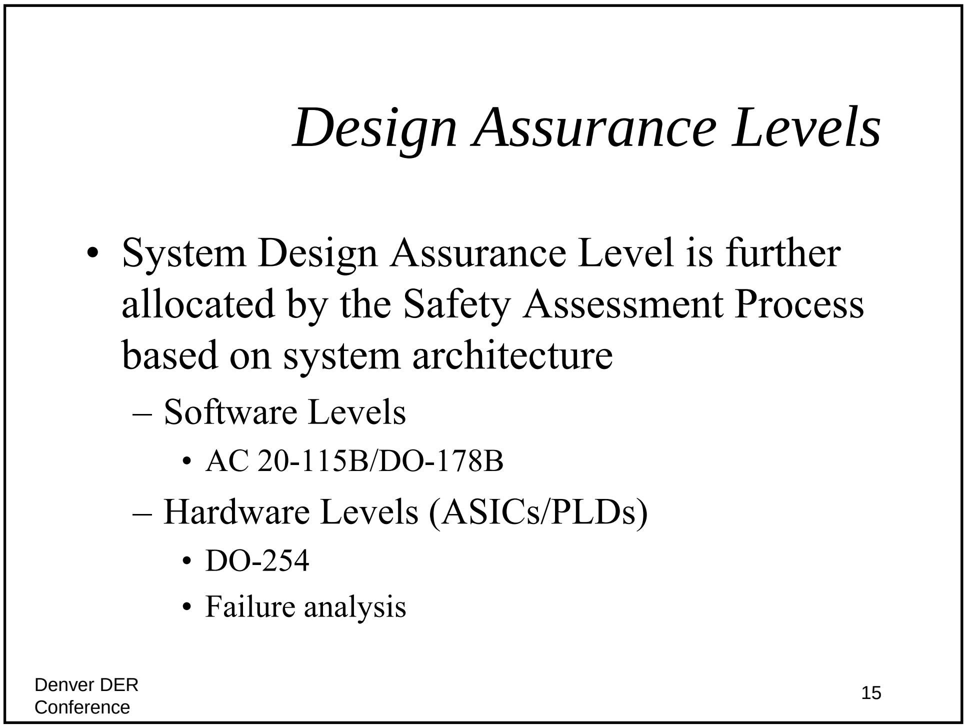


Design Assurance Levels

- Why ??
  - – Avionics systems present opportunities for development error(s)
  - – Not practical or possible to develop a finite test suite to determine residual development error(s)
  - – Errors can be non-deterministic and are not easily characterized
  - – Obtain design approvals for intended function

Denver DER
Conference

14

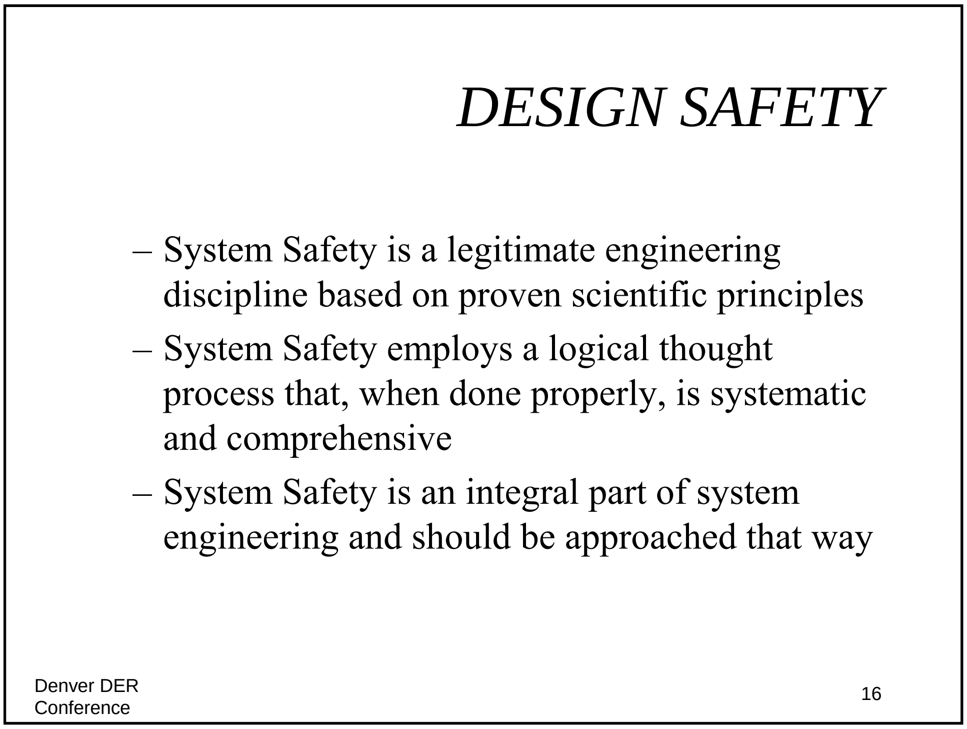


Design Assurance Levels

- System Design Assurance Level is further allocated by the Safety Assessment Process based on system architecture
  - – Software Levels
    - AC 20-115B/DO-178B
  - – Hardware Levels (ASICs/PLDs)
    - DO-254
    - Failure analysis

Denver DER
Conference

15

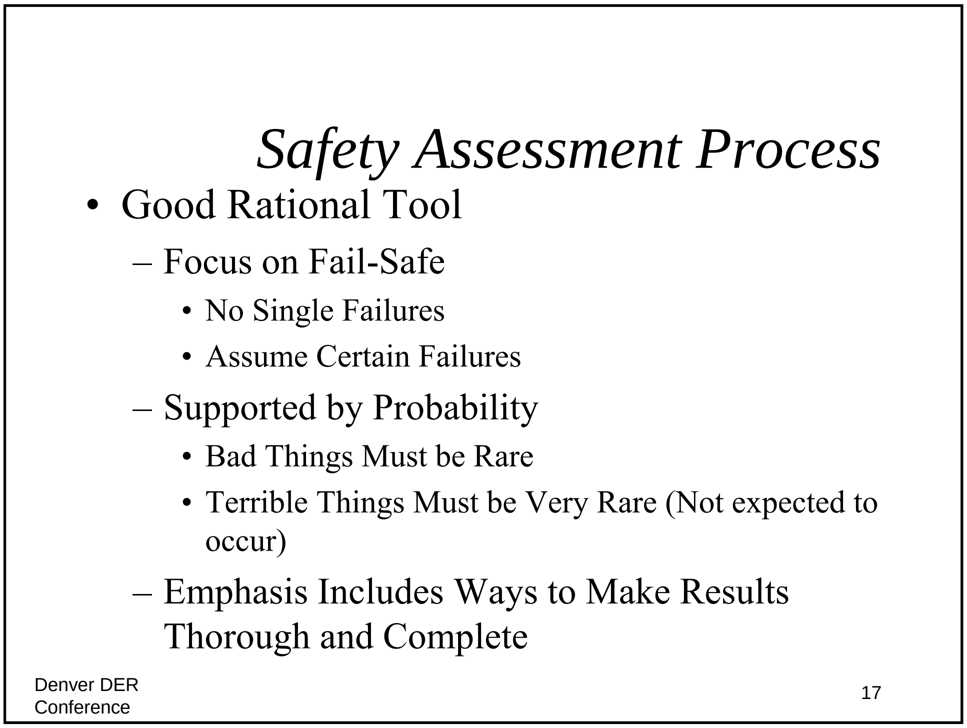


DESIGN SAFETY

- – System Safety is a legitimate engineering discipline based on proven scientific principles
- – System Safety employs a logical thought process that, when done properly, is systematic and comprehensive
- – System Safety is an integral part of system engineering and should be approached that way

Denver DER
Conference

16

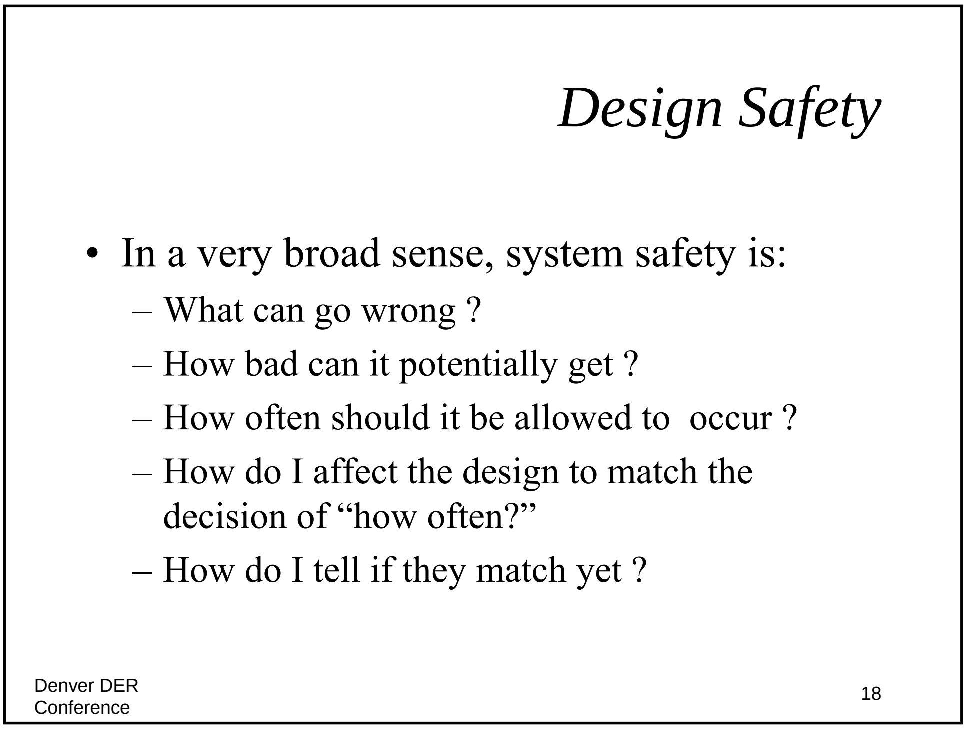


Safety Assessment Process

- Good Rational Tool
  - Focus on Fail-Safe
    - No Single Failures
    - Assume Certain Failures
  - Supported by Probability
    - Bad Things Must be Rare
    - Terrible Things Must be Very Rare (Not expected to occur)
  - Emphasis Includes Ways to Make Results Thorough and Complete

Denver DER
Conference

17

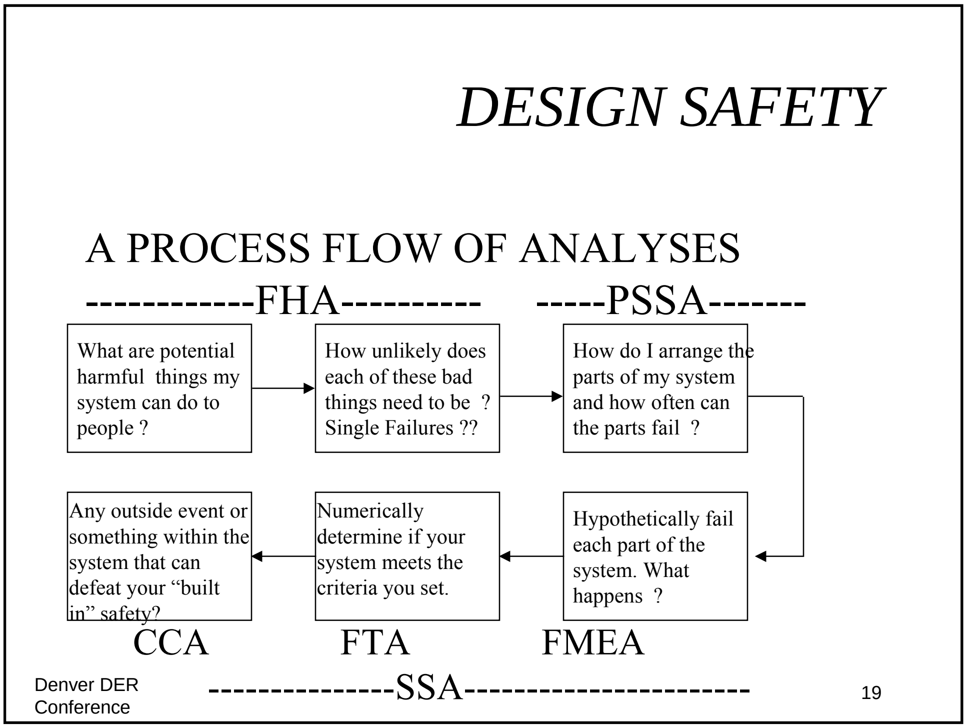


Design Safety

- In a very broad sense, system safety is:
  - What can go wrong ?
  - How bad can it potentially get ?
  - How often should it be allowed to occur ?
  - How do I affect the design to match the decision of “how often?”
  - How do I tell if they match yet ?

Denver DER
Conference

18



DESIGN SAFETY

A PROCESS FLOW OF ANALYSES

------------FHA----------   -----PSSA-------

What are potential harmful things my system can do to people ?

How unlikely does each of these bad things need to be ? Single Failures ??

How do I arrange the parts of my system and how often can the parts fail ?

Hypothetically fail each part of the system. What happens ?

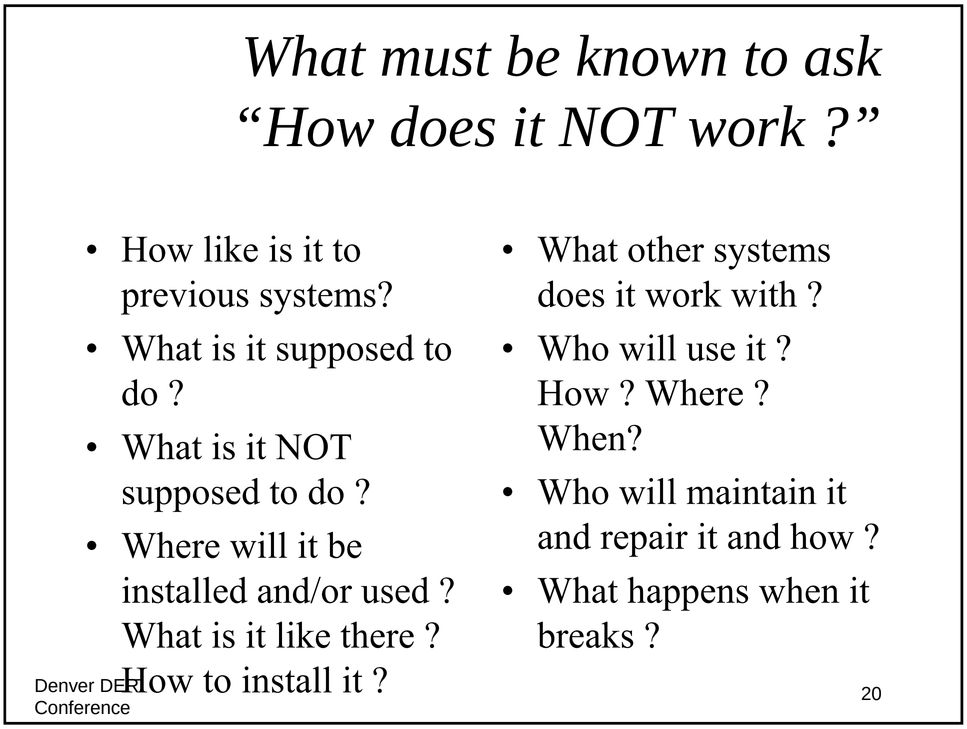
Numerically determine if your system meets the criteria you set.

Any outside event or something within the system that can defeat your "built in" safety?

CCA   FTA   FMEA

---------------SSA----------------------

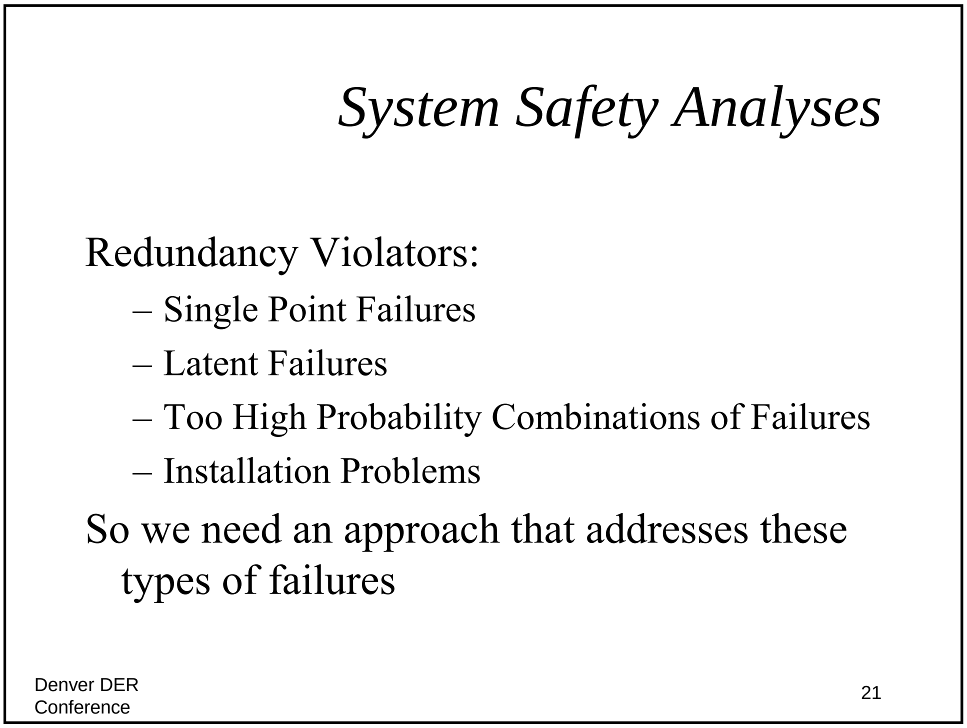
Denver DER Conference   19



What must be known to ask "How does it NOT work ?"

- How like is it to previous systems?
- What is it supposed to do ?
- What is it NOT supposed to do ?
- Where will it be installed and/or used ? What is it like there ? How to install it ?
- What other systems does it work with ?
- Who will use it ? How ? Where ? When?
- Who will maintain it and repair it and how ?
- What happens when it breaks ?

Denver DER Conference   20

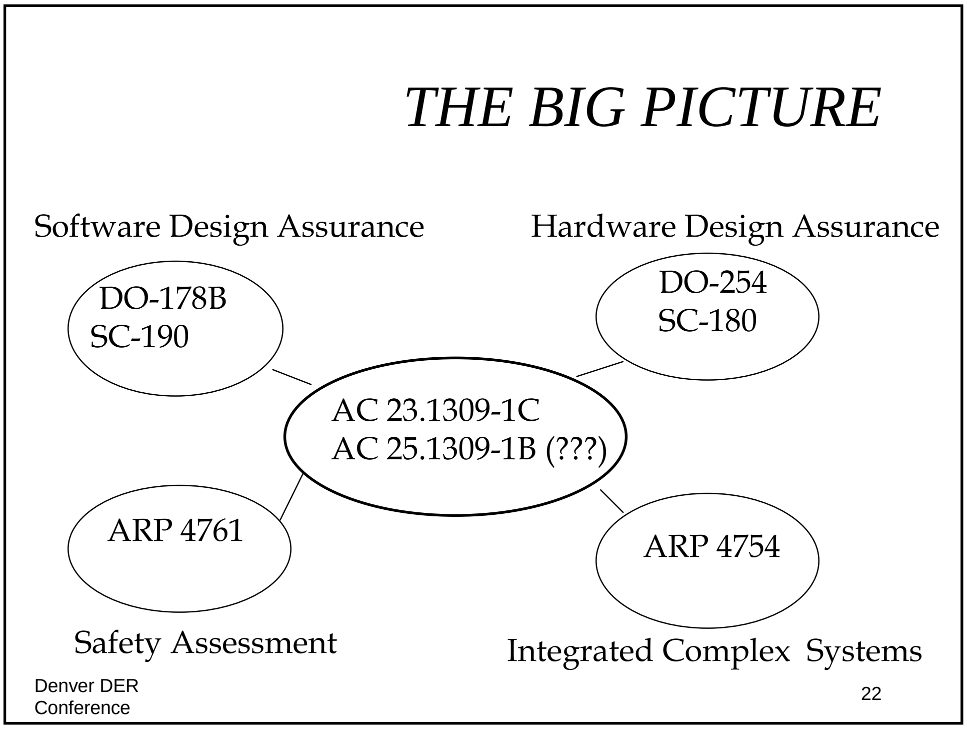


System Safety Analyses

Redundancy Violators:

- Single Point Failures
- Latent Failures
- Too High Probability Combinations of Failures
- Installation Problems

So we need an approach that addresses these types of failures



THE BIG PICTURE

Software Design Assurance

DO-178B
SC-190

Hardware Design Assurance

DO-254
SC-180

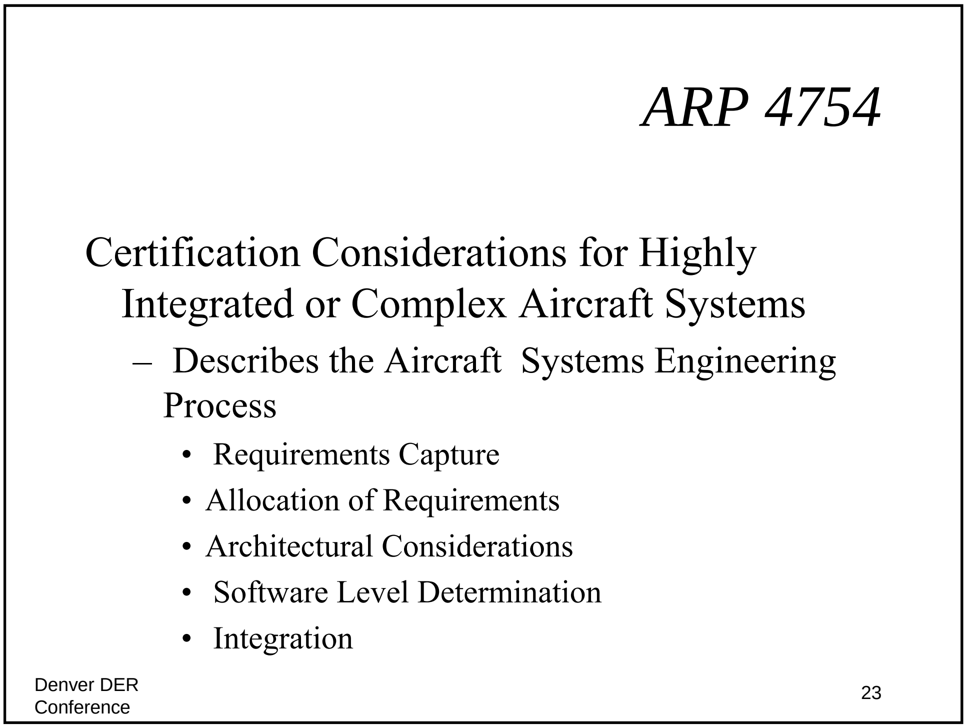
AC 23.1309-1C
AC 25.1309-1B (???)

ARP 4761

Safety Assessment

ARP 4754

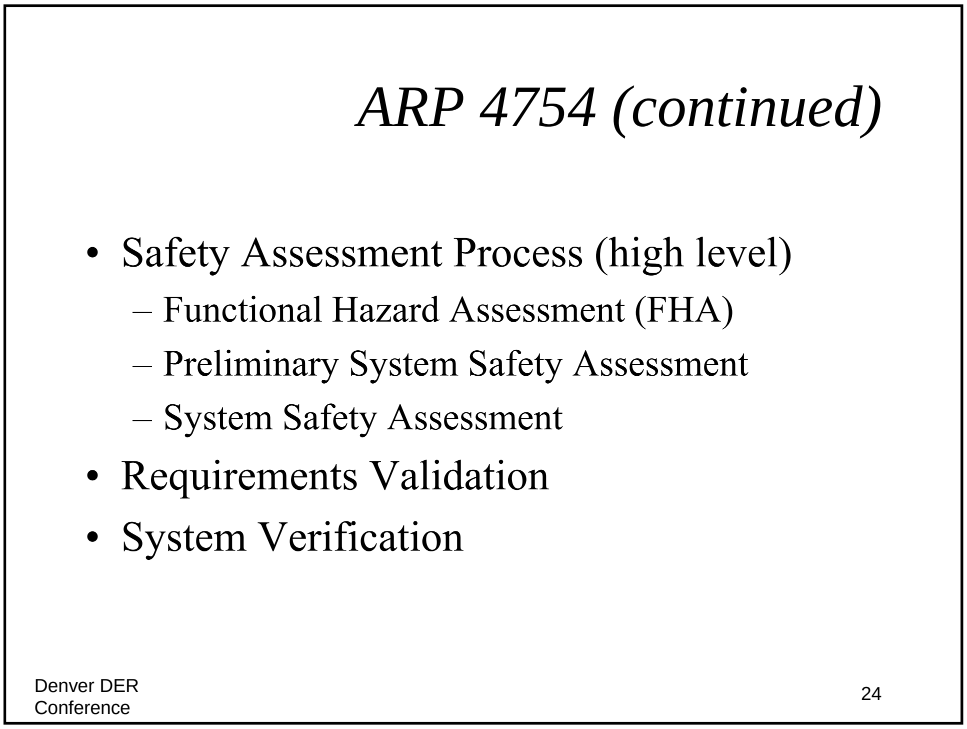
Integrated Complex Systems



ARP 4754

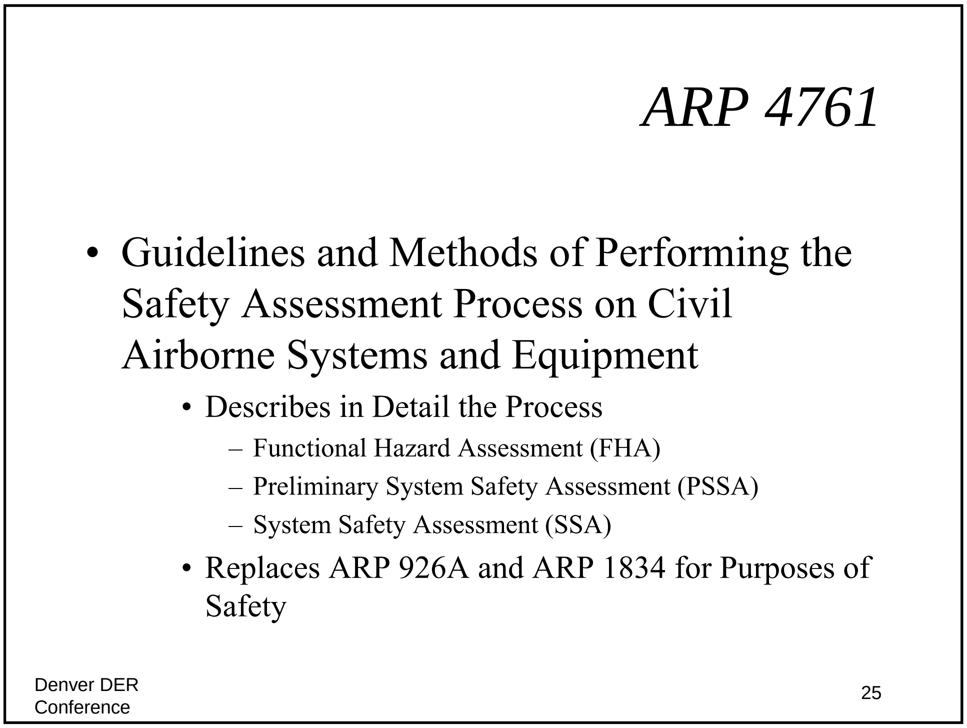
Certification Considerations for Highly Integrated or Complex Aircraft Systems

- Describes the Aircraft Systems Engineering Process
  - Requirements Capture
  - Allocation of Requirements
  - Architectural Considerations
  - Software Level Determination
  - Integration



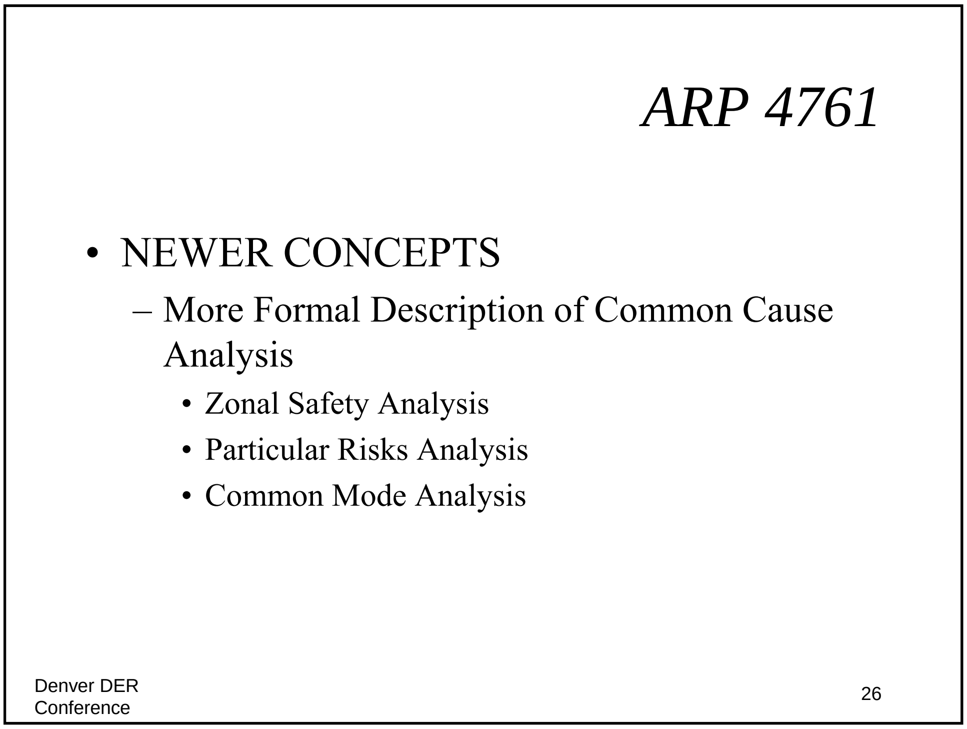
ARP 4754 (continued)

- Safety Assessment Process (high level)
  - Functional Hazard Assessment (FHA)
  - Preliminary System Safety Assessment
  - System Safety Assessment
- Requirements Validation
- System Verification



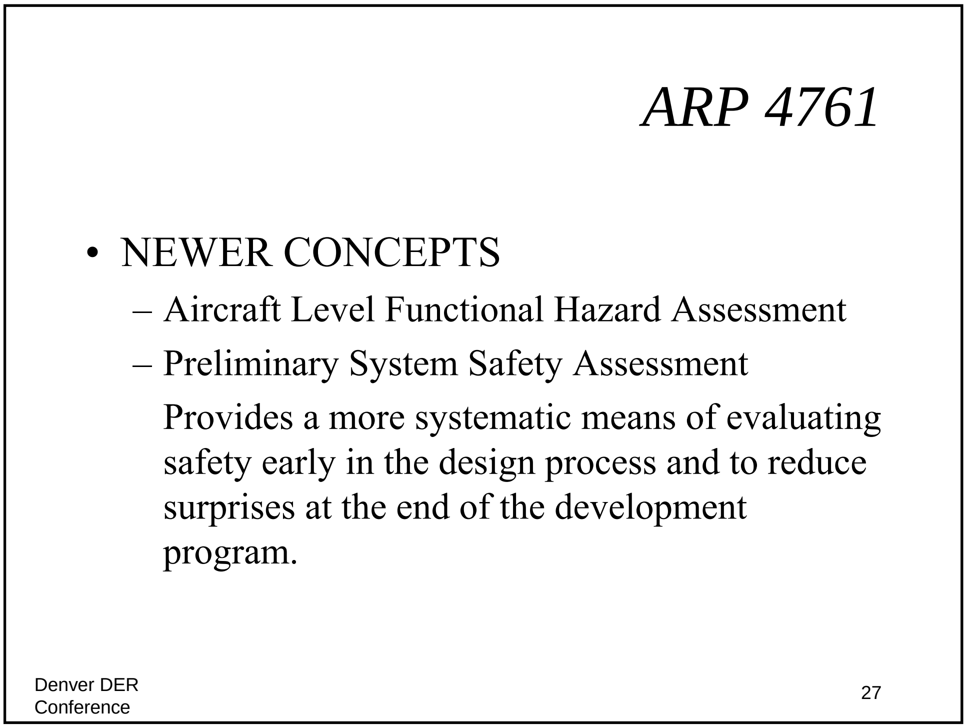
ARP 4761

- Guidelines and Methods of Performing the Safety Assessment Process on Civil Airborne Systems and Equipment
    - Describes in Detail the Process
        - Functional Hazard Assessment (FHA)
        - Preliminary System Safety Assessment (PSSA)
        - System Safety Assessment (SSA)
    - Replaces ARP 926A and ARP 1834 for Purposes of Safety



ARP 4761

- NEWER CONCEPTS
    - More Formal Description of Common Cause Analysis
        - Zonal Safety Analysis
        - Particular Risks Analysis
        - Common Mode Analysis



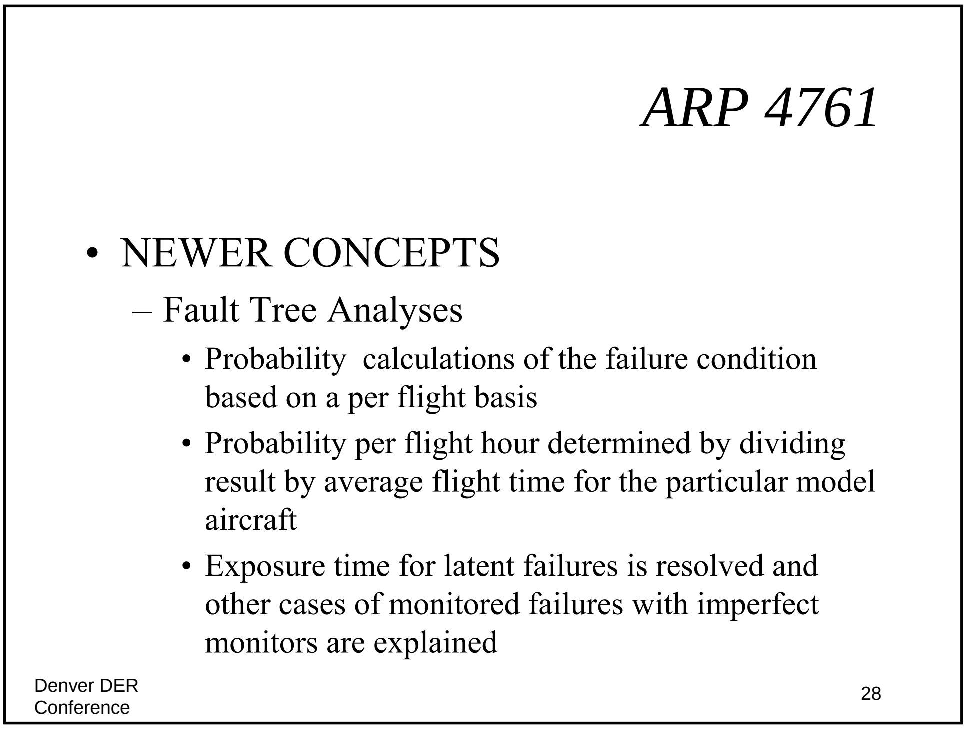
ARP 4761

- NEWER CONCEPTS
  - Aircraft Level Functional Hazard Assessment
  - Preliminary System Safety Assessment

    Provides a more systematic means of evaluating safety early in the design process and to reduce surprises at the end of the development program.

Denver DER
Conference

27

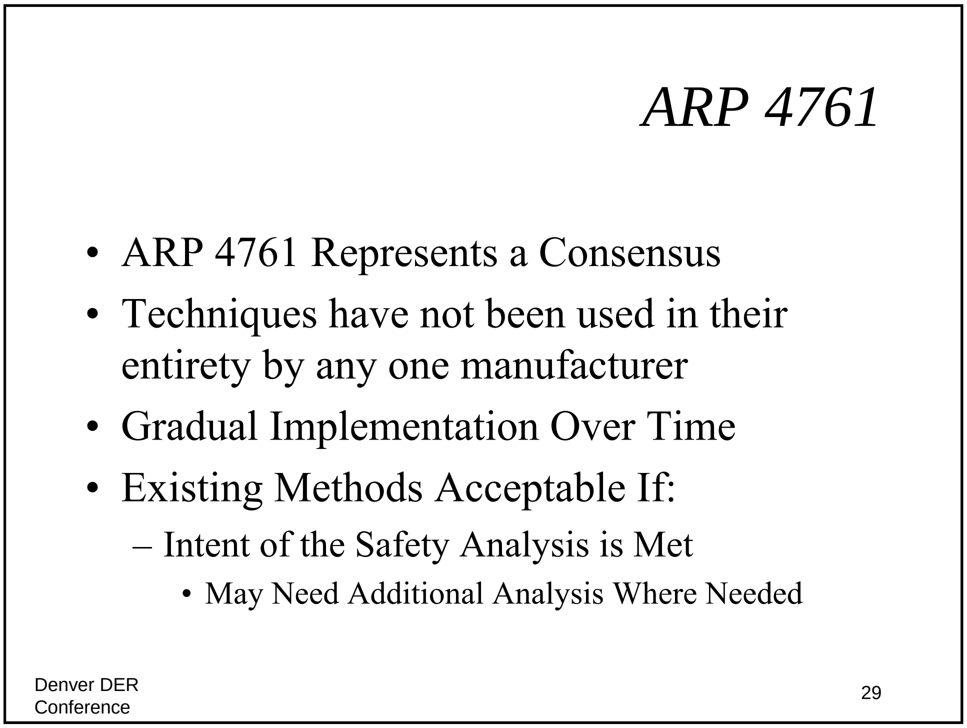


ARP 4761

- NEWER CONCEPTS
  - Fault Tree Analyses
    - Probability calculations of the failure condition based on a per flight basis
    - Probability per flight hour determined by dividing result by average flight time for the particular model aircraft
    - Exposure time for latent failures is resolved and other cases of monitored failures with imperfect monitors are explained

Denver DER
Conference

28

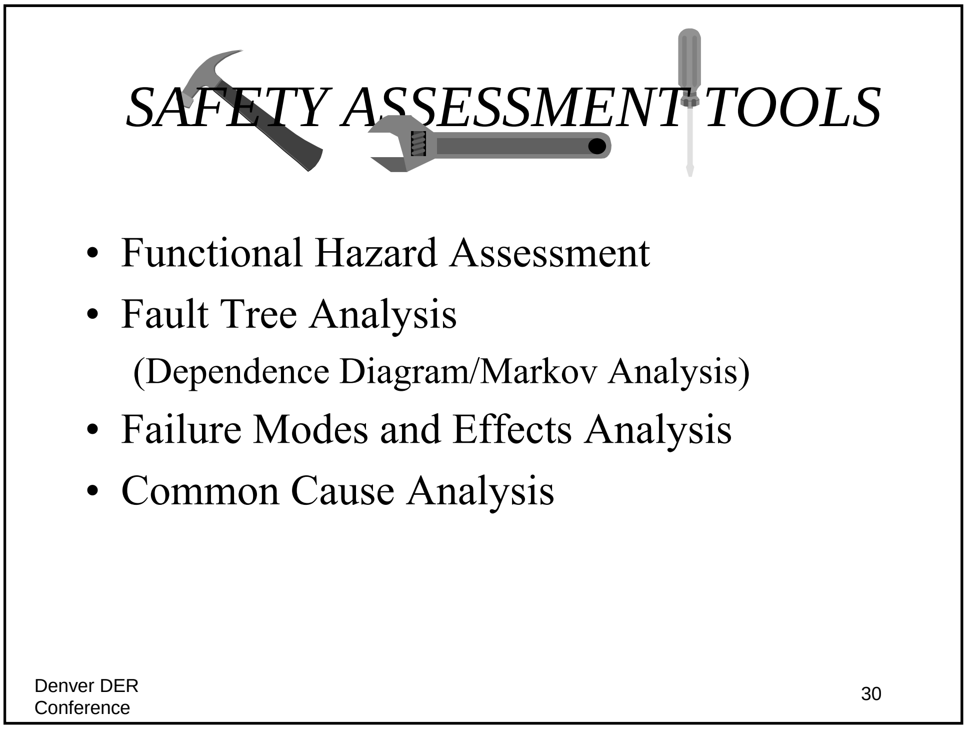


ARP 4761

- ARP 4761 Represents a Consensus
- Techniques have not been used in their entirety by any one manufacturer
- Gradual Implementation Over Time
- Existing Methods Acceptable If:
  - Intent of the Safety Analysis is Met
    - May Need Additional Analysis Where Needed

Denver DER
Conference

29



SAFETY ASSESSMENT TOOLS

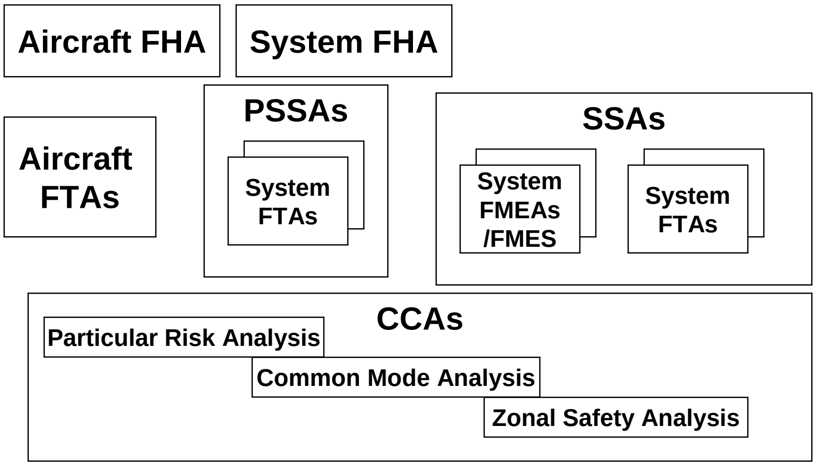
- Functional Hazard Assessment
- Fault Tree Analysis

  (Dependence Diagram/Markov Analysis)
- Failure Modes and Effects Analysis
- Common Cause Analysis

Denver DER
Conference

30

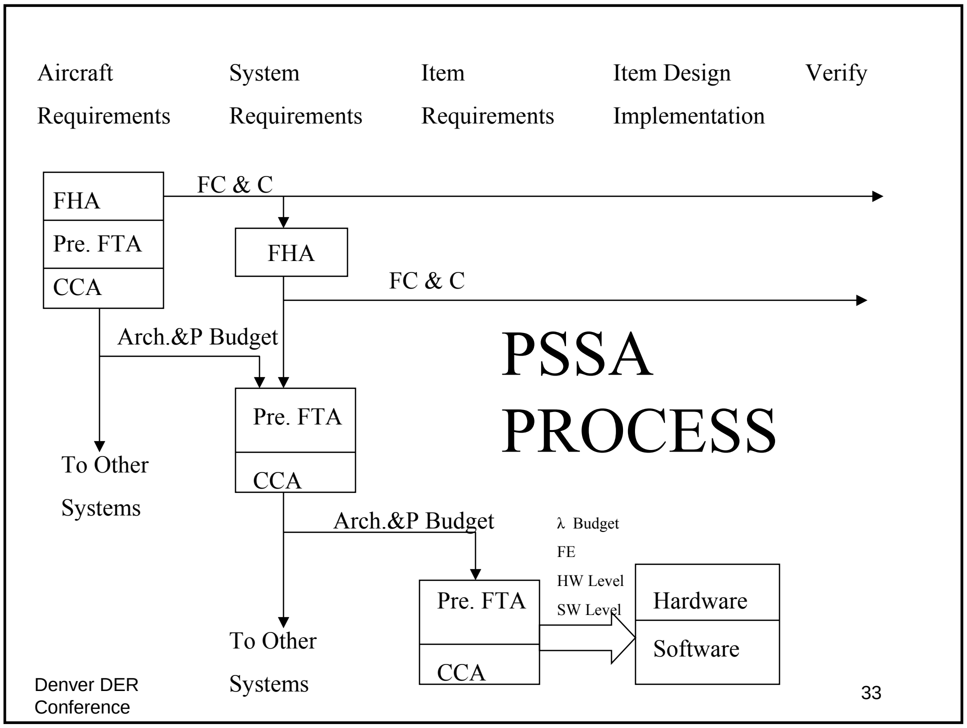
Safety Assessment Process Overview



PSSA

DEFINITION:

A system evaluation of the proposed architecture(s) and implementation(s) based on the Functional Hazard Assessment (FHA) failure condition classifications to determine safety requirements of the system.



Aircraft Requirements

System Requirements

Item Requirements

Item Design Implementation

Verify

FHA

Pre. FTA

CCA

FC & C

FHA

FC & C

Arch.&P Budget

PSSA PROCESS

Pre. FTA

CCA

To Other Systems

Arch.&P Budget

λ Budget

FE

HW Level

SW Level

Pre. FTA

CCA

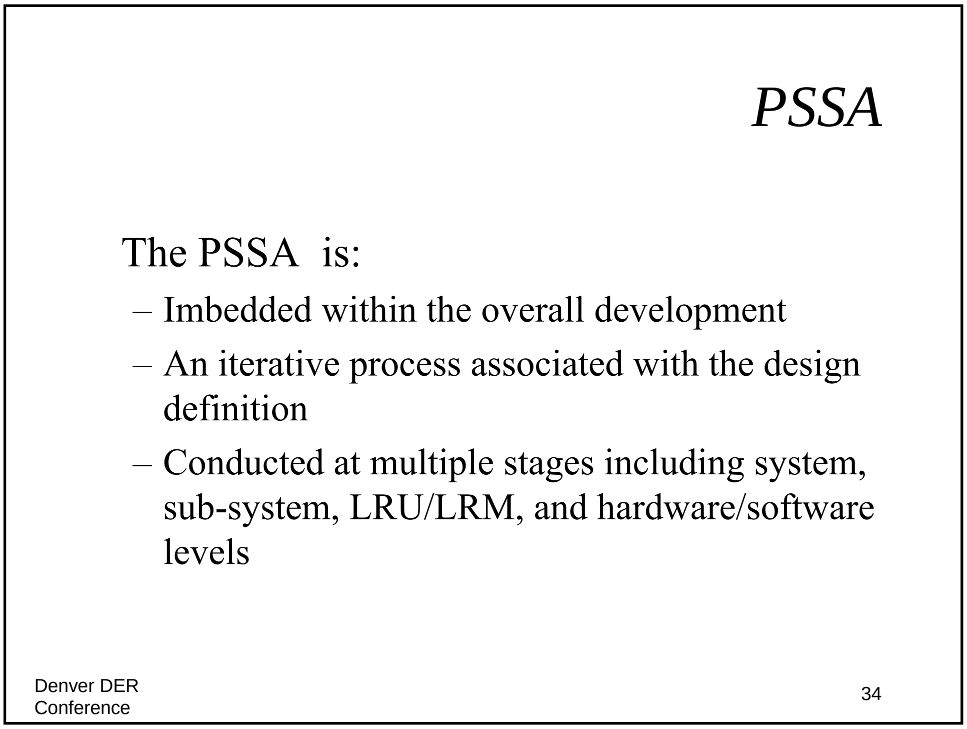
Hardware

Software

To Other Systems

Denver DER Conference

33



PSSA

The PSSA is:

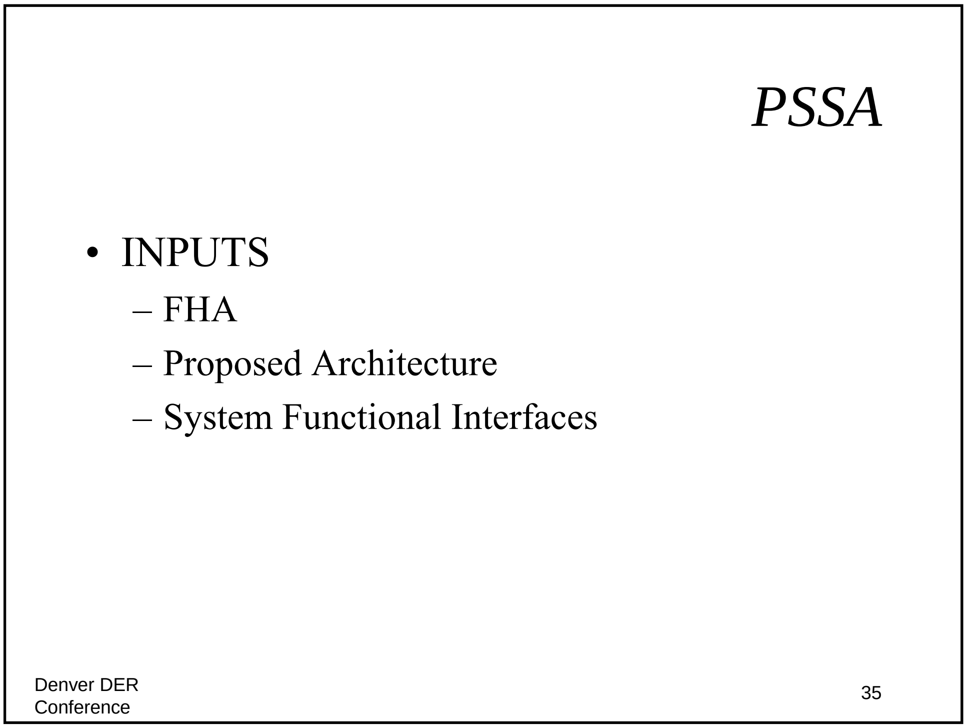
– Imbedded within the overall development

– An iterative process associated with the design definition

– Conducted at multiple stages including system, sub-system, LRU/LRM, and hardware/software levels

Denver DER Conference

34

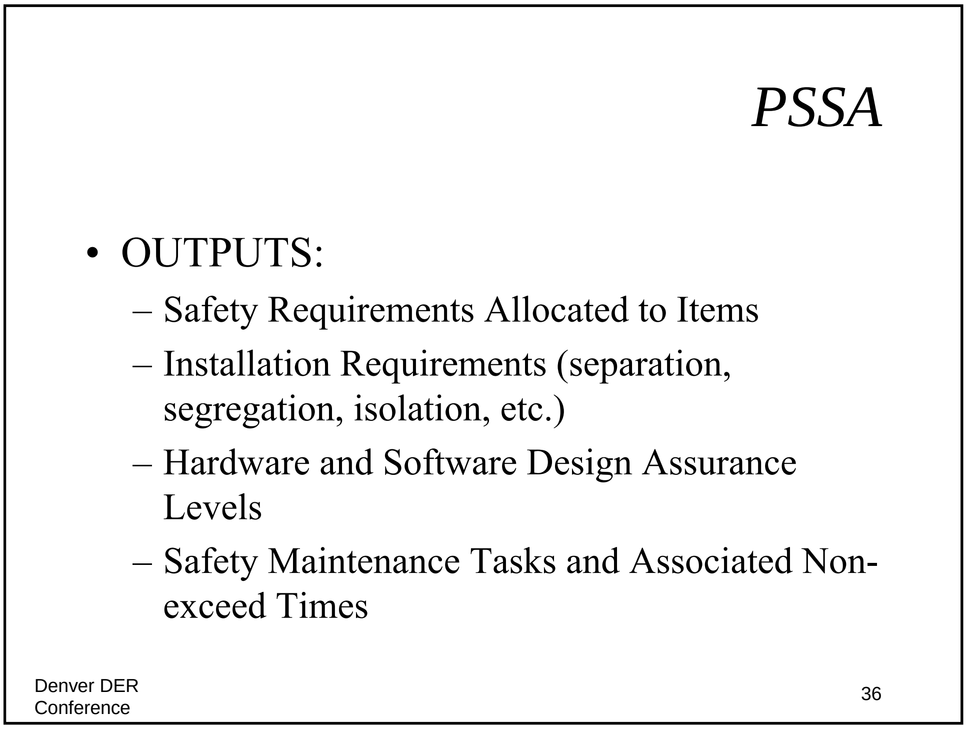


PSSA

- INPUTS
  - – FHA
  - – Proposed Architecture
  - – System Functional Interfaces

Denver DER
Conference

35

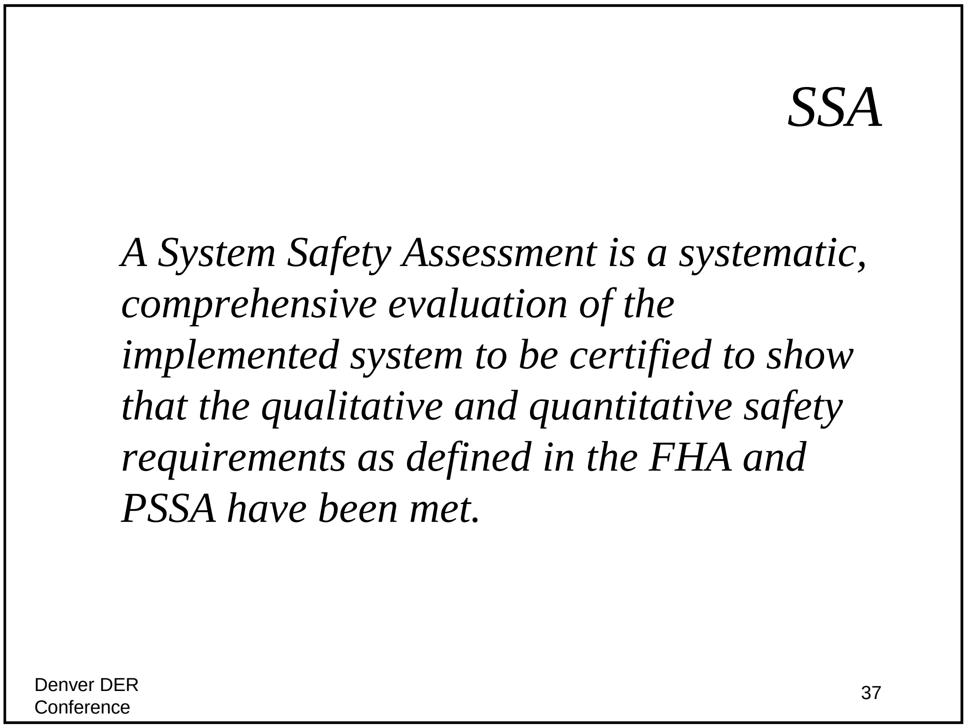


PSSA

- OUTPUTS:
  - – Safety Requirements Allocated to Items
  - – Installation Requirements (separation, segregation, isolation, etc.)
  - – Hardware and Software Design Assurance Levels
  - – Safety Maintenance Tasks and Associated Non-exceed Times

Denver DER
Conference

36

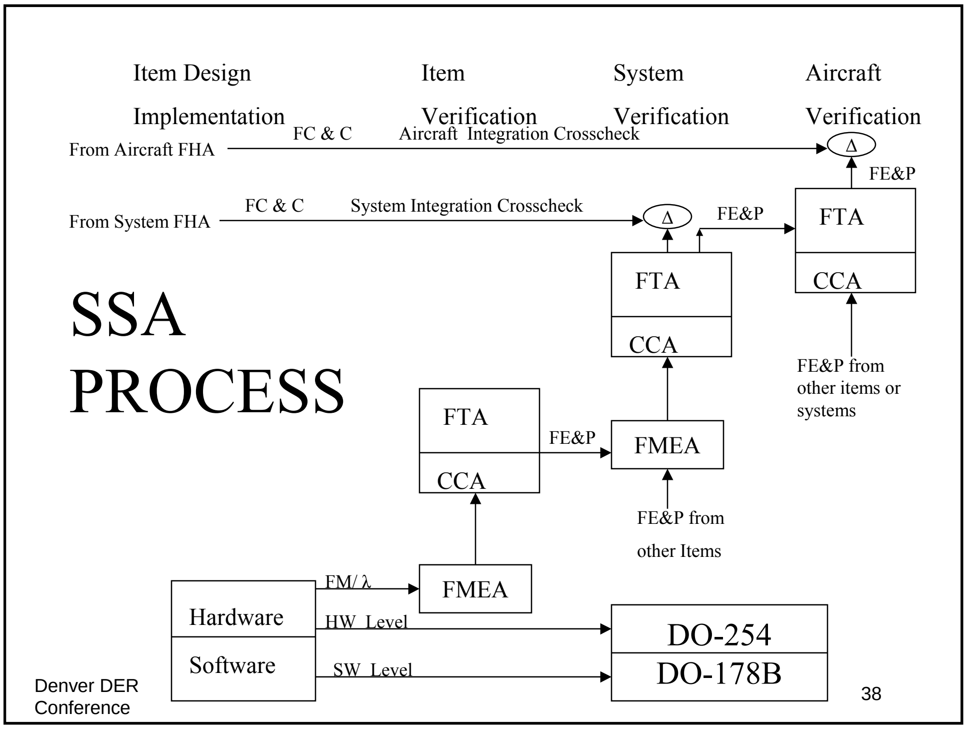


SSA

A System Safety Assessment is a systematic, comprehensive evaluation of the implemented system to be certified to show that the qualitative and quantitative safety requirements as defined in the FHA and PSSA have been met.

Denver DER
Conference

37



SSA PROCESS

Item Design Implementation

Item Verification

System Verification

Aircraft Verification

From Aircraft FHA

FC & C

Aircraft Integration Crosscheck

Δ

FE&P

From System FHA

FC & C

System Integration Crosscheck

Δ

FE&P

FTA

CCA

FTA

CCA

FE&P from other items or systems

FTA

CCA

FE&P

FMEA

FE&P from

other Items

FM/ λ

FMEA

Hardware

Software

HW Level

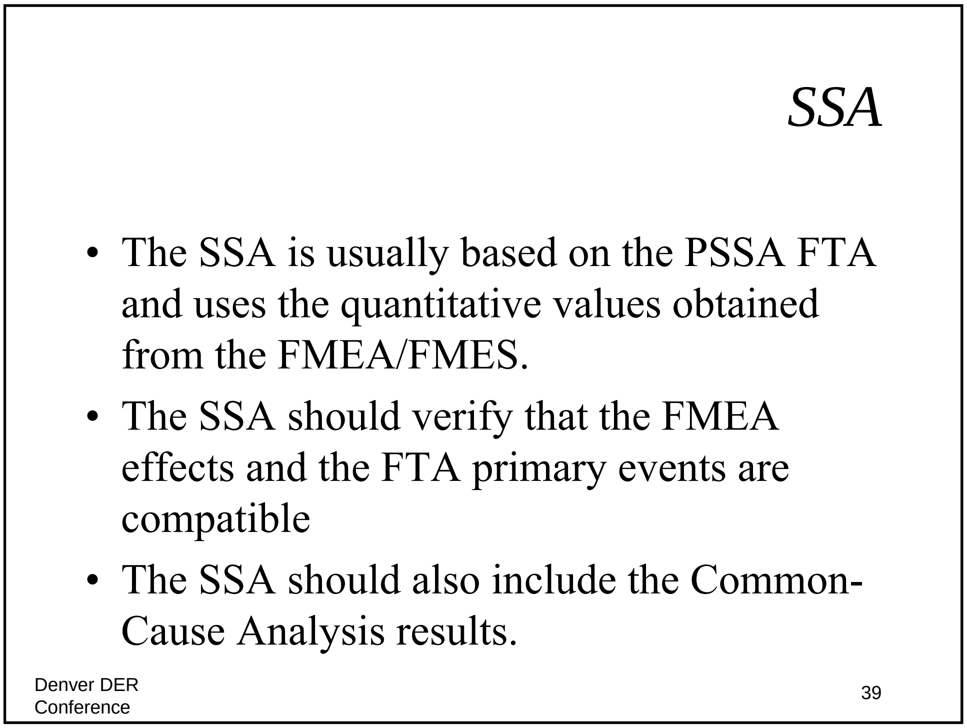
SW Level

DO-254

DO-178B

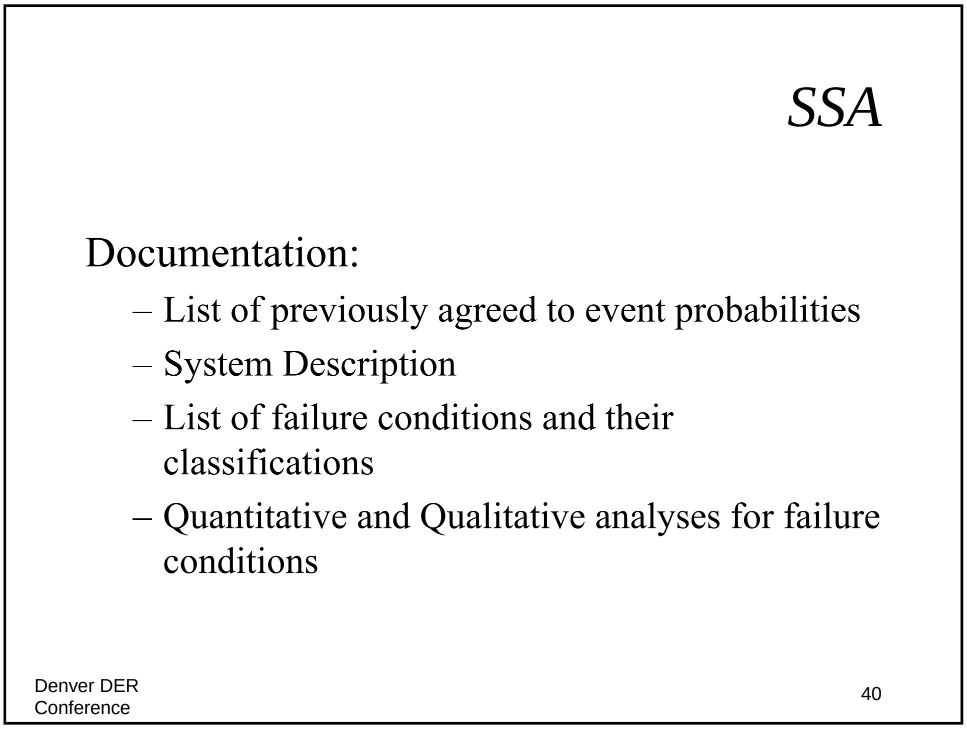
Denver DER
Conference

38



SSA

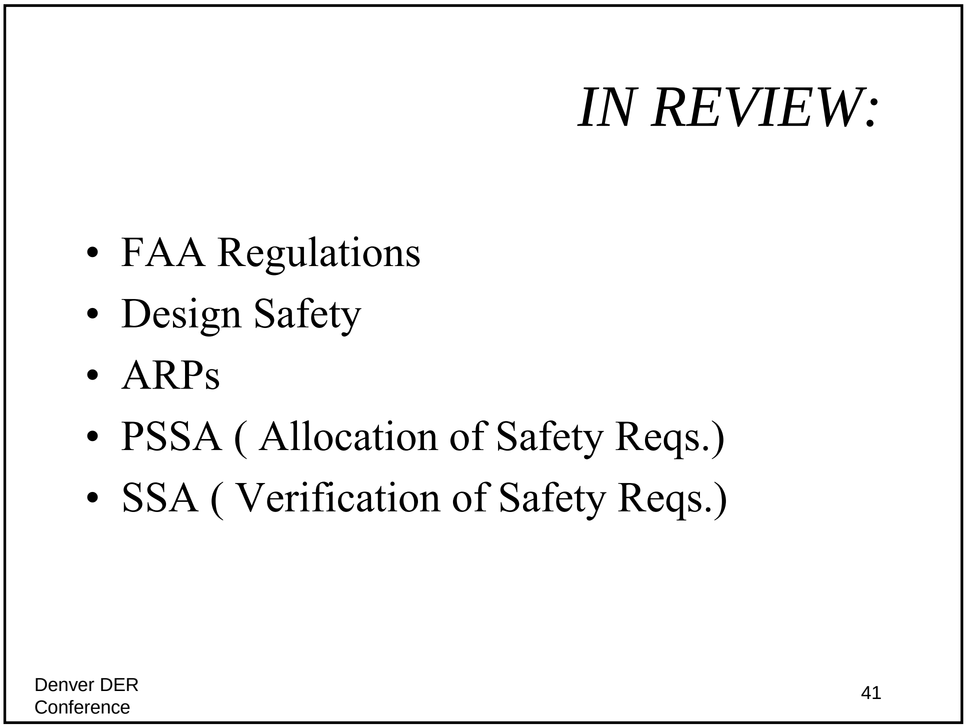
- The SSA is usually based on the PSSA FTA and uses the quantitative values obtained from the FMEA/FMES.
- The SSA should verify that the FMEA effects and the FTA primary events are compatible
- The SSA should also include the Common-Cause Analysis results.



SSA

Documentation:

- List of previously agreed to event probabilities
- System Description
- List of failure conditions and their classifications
- Quantitative and Qualitative analyses for failure conditions

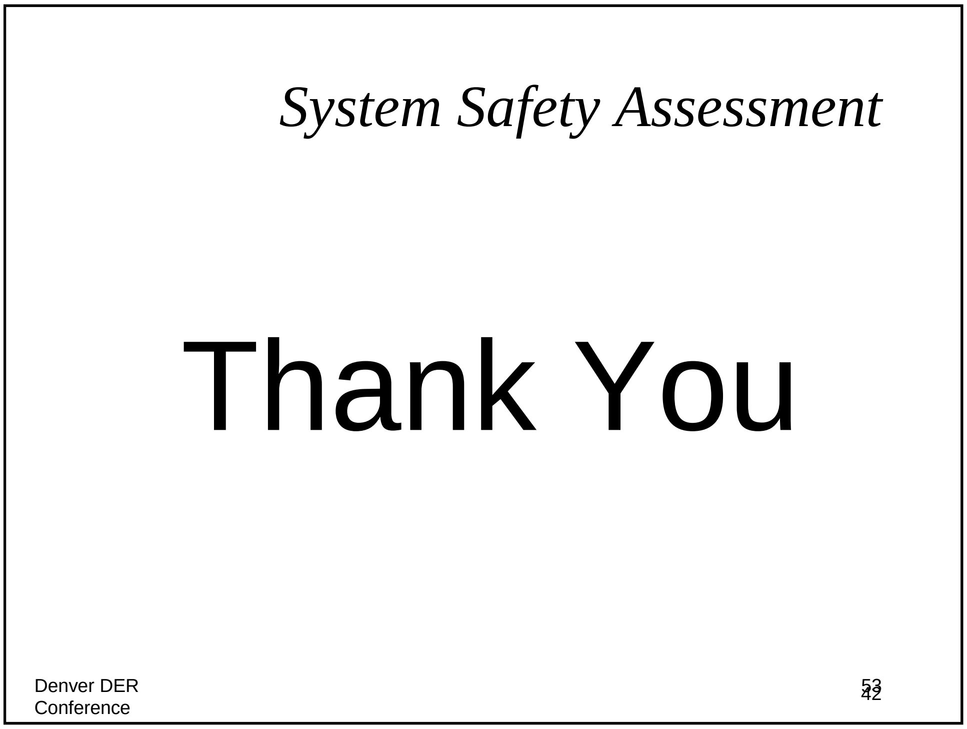


IN REVIEW:

- FAA Regulations
- Design Safety
- ARPs
- PSSA (Allocation of Safety Reqs.)
- SSA (Verification of Safety Reqs.)

Denver DER
Conference

41



System Safety Assessment

Thank You

Denver DER
Conference

53
42